14 Cryptography Basics

🔐 Cryptography & Password Cracking

1. What is Cryptography in Cybersecurity?

- Cryptography is the **science of securing information** by transforming it into a format that is unreadable to unauthorized users.
- It ensures **confidentiality, integrity, authenticity, and non-repudiation** of data.
- Core to protecting communication, data storage, authentication, and digital signatures.

2. What are the Different Types of Cryptography?

- **Symmetric Cryptography:** Same key used for encryption and decryption (e.g., AES, DES).
- **Asymmetric Cryptography:** Uses a pair of keys — public key for encryption and private key for decryption (e.g., RSA, ECC).
- **Hash Functions:** Generate fixed-length output (digest) from data, used for integrity (e.g., SHA-256, MD5).
- **Hybrid Cryptography:** Combines symmetric and asymmetric to benefit from both.

3. What is Encryption?

- The process of **converting plaintext into ciphertext** using an algorithm and an encryption key, making data unreadable without the corresponding key.

4. What is Decryption?

- The reverse process of encryption: **transforming ciphertext back into readable plaintext** using a decryption key.

5. What is the Importance of Cryptography?

- Protects sensitive data from unauthorized access.
- Enables secure communication over insecure channels (e.g., internet).
- Provides **authentication** and **data integrity** guarantees.
- Enables **digital signatures** and **non-repudiation** for legal and audit trails.

6. What are the Types of Cryptography? *(Reinforcement)*

- **Symmetric Key Algorithms:** Fast, used for bulk data encryption.
- **Asymmetric Key Algorithms:** Used for key exchange, digital signatures.
- **Hashing:** One-way functions for verifying integrity, password storage.

- **Steganography:** Hiding data inside other files (less common but related).

---

7. What are the Applications of Cryptography?

- Secure communication protocols (TLS/SSL).
- Email encryption (PGP, S/MIME).
- Disk encryption (BitLocker, LUKS).
- Password hashing and authentication.
- Blockchain and cryptocurrencies.
- Digital signatures and certificate authorities.

---

8. What is a Hash Algorithm?

- A **hash algorithm** takes an input of any size and produces a fixed-size output (hash or digest).
- It is **one-way:** practically impossible to revert hash to original input.
- Used for verifying data integrity and storing passwords securely.

---

9. What Does SHA Stand For?

- **SHA = Secure Hash Algorithm**
- A family of cryptographic hash functions designed by the NSA.
- Variants: SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3.
- SHA-256 is widely used due to better security than SHA-1 or MD5.

---

10. What is John the Ripper?

- John the Ripper (JtR) is an **open-source password cracking tool**.
- It performs **dictionary attacks, brute force, and hybrid attacks** on password hashes.
- Supports many hash types (UNIX, Windows, MD5, SHA, etc.).

---

11. How to Use John the Ripper?

- Basic command: `john <hashfile>` – automatically detects hash format and starts cracking.
- Use **wordlists** for dictionary attacks: `john --wordlist=rockyou.txt <hashfile>`
- Customize rules and brute force with additional options.
- Use `john --show <hashfile>` to see cracked passwords.

---

12. How to Crack Advanced Hashes with John the Ripper?

- Use **“Jumbo” version** of John with extended hash support (bcrypt, WPA, etc.).
- Utilize **rulesets and masks** to optimize attacks.
- Combine **wordlists + incremental brute force** for better coverage.

- Employ **parallel processing or GPU acceleration** for performance.

---

13. What is Hashcat?

- Hashcat is a **powerful, GPU-accelerated password cracking tool**.
- Supports a wide range of hash algorithms and cracking modes (dictionary, brute-force, combinator, rule-based).
- Known for speed and versatility in cracking complex hashes.

---

14. How to Use Hashcat?

- Basic syntax: `hashcat -m <hash_mode> -a <attack_mode> <hashfile> <wordlist>`
  - `-m` specifies hash type (e.g., 0 for MD5, 100 for SHA1).
  - `-a` specifies attack mode (0 = dictionary, 3 = brute force).
- Example: `hashcat -m 0 -a 0 hashes.txt rockyou.txt` (cracks MD5 hashes with rockyou wordlist)
- Use rules to modify wordlists and mask attacks for targeted guessing.
- Monitor progress and resume cracked sessions with options.
